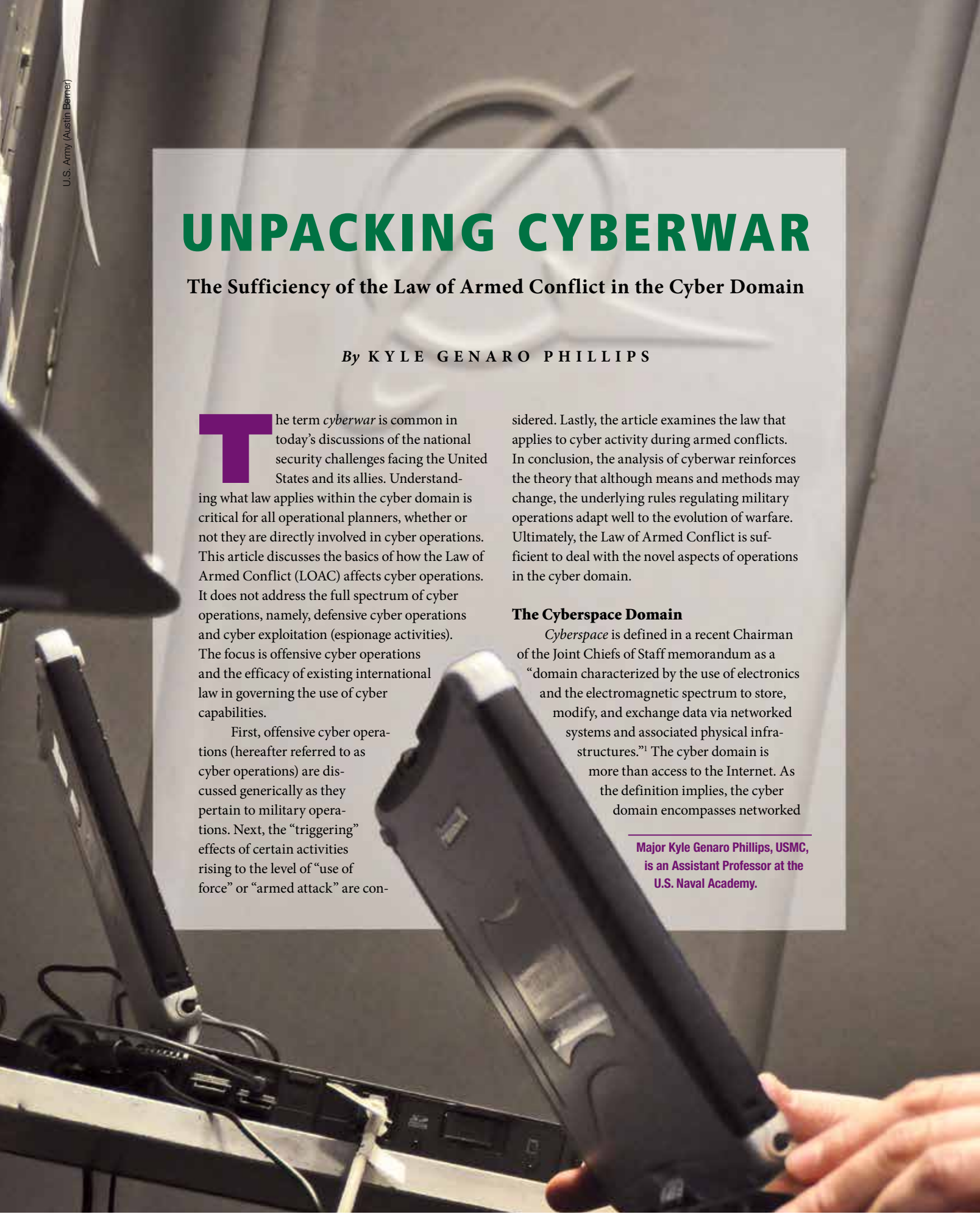


U.S. Army (Austin Berner)

UNPACKING CYBERWAR

The Sufficiency of the Law of Armed Conflict in the Cyber Domain

By KYLE GENARO PHILLIPS

The term *cyberwar* is common in today's discussions of the national security challenges facing the United States and its allies. Understanding what law applies within the cyber domain is critical for all operational planners, whether or not they are directly involved in cyber operations. This article discusses the basics of how the Law of Armed Conflict (LOAC) affects cyber operations. It does not address the full spectrum of cyber operations, namely, defensive cyber operations and cyber exploitation (espionage activities). The focus is offensive cyber operations and the efficacy of existing international law in governing the use of cyber capabilities.

First, offensive cyber operations (hereafter referred to as cyber operations) are discussed generically as they pertain to military operations. Next, the "triggering" effects of certain activities rising to the level of "use of force" or "armed attack" are considered. Lastly, the article examines the law that applies to cyber activity during armed conflicts. In conclusion, the analysis of cyberwar reinforces the theory that although means and methods may change, the underlying rules regulating military operations adapt well to the evolution of warfare. Ultimately, the Law of Armed Conflict is sufficient to deal with the novel aspects of operations in the cyber domain.

The Cyberspace Domain

Cyberspace is defined in a recent Chairman of the Joint Chiefs of Staff memorandum as a "domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."[1] The cyber domain is more than access to the Internet. As the definition implies, the cyber domain encompasses networked

Major Kyle Genaro Phillips, USMC, is an Assistant Professor at the U.S. Naval Academy.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Unpacking Cyberwar: The Sufficiency of the Law of Armed Conflict in the Cyber Domain	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Joint Force Quarterly ,260 Fifth Avenue, Building 64, Fort Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

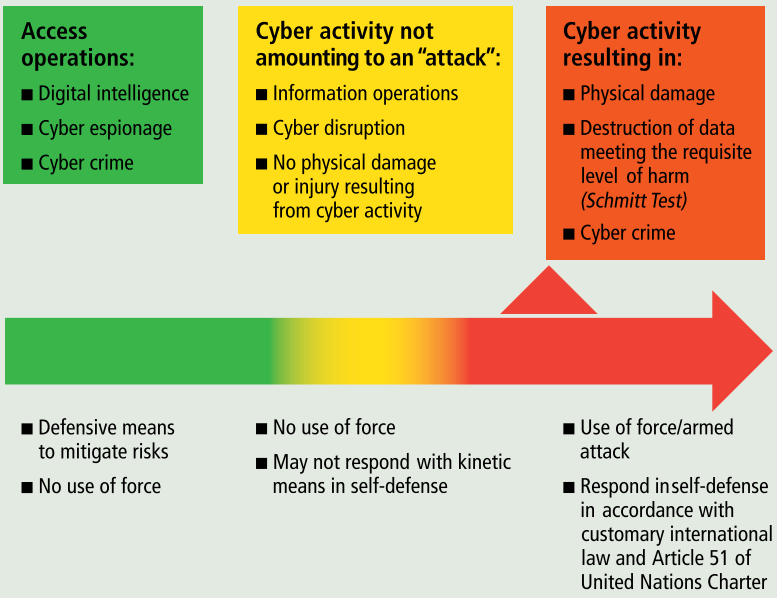
15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**6**	

U.S. Air Force (Leah Young)

Airmen discuss Joint Precision Airdrop System prior to mission at Joint Base Lewis-McChord, Washington, using GPS to guide cargo to drop zone

Figure. Spectrum of Cyber Operations*



*Adapted from brief provided by LCDR Paul Walker, USN, JAGC

systems regardless of whether those systems are publicly accessed. Additionally, the cyber domain is a manmade physical entity and must be distinguished from operations performed within the domain itself. For example, information operations may be performed within the cyber domain but also through other domains of land, sea, and air as evidenced by the dropping of leaflets, personal engagements of key leaders with local populations, and public broadcasts.[2]

For purposes of the application of the LOAC, it is important to separate operations conducted exclusively in the cyber domain from operations in which cyber activity supports larger military efforts. Two examples from Richard Clarke's *Cyber War* illustrate the distinction.

First, the Estonia cyber event in 2007, although not officially attributed to the Russian government, involved attacking "botnets" resident in "zombie" computers that created a flood of cyber access requests. The distributed denial-of-service (DDOS) attacks led to the collapse of online banking, newspaper Web sites, and government electronic services within the state.[3] The DDOS activity was conducted during a heated political dispute between the Russian government and Estonia. A bronze statue was erected in Estonia recognizing the Red Army's efforts in "liberating" the Estonian population from the Nazis after World War II. The dispute over the statue involved Estonian legislation calling for the removal of the statue due to the increasing resentment by the population over the history of Soviet control following the war. The legislation was subsequently vetoed by the Estonian president in response to intense political pressure from Moscow. However, nationalists continued to call for the removal or destruction of the statue. The dispute moved into the cyber domain where the DDOS activity temporarily crippled the population.[4] The activity against Estonia is an example of utilizing a cyber capability as the *primary tool* during a dispute.

Next, compare the Estonian case to an event involving Syria and Israel the same year. According to Clarke, the Israeli military utilized a cyber tool to control the detection systems in the Syrian air defense. The result was a radar picture that displayed only what the Israeli military wanted the Syrians to see. After the air defense systems were "owned" by the Israeli military, attack aircraft flew in and bombed a suspected nuclear weapons plant. Despite a number of contrary accounts of the event, if true, the raid on Syria is an example of utilizing a cyber tool as a *supporting effort* to a traditional military operation.[5]

Cyber Activity and *Jus Ad Bellum*

Jus ad bellum is the international law governing a state's use of force and is based on the customary international law principle of a state's inherent right of self-defense. It is codified in Article 51 of the United Nations (UN) Charter governing individual and collective self-defense.[6] The threshold question that must be answered to determine what law may apply to military cyber activity conducted by a state is whether an armed conflict exists between a state and adversary, be that adversary a state or nonstate actor. Jus ad bellum provides a starting point for the analysis on the lawful use of cyber activity by a state's military.

Article 2(4) of the UN Charter prohibits the threat or use of force by member states in their international relations against the territorial integrity or political independence of any state.[7] As specified above, Article 51 recognizes a state's inherent right to individual and collective self-defense against an *armed attack*. The International Court of Justice in the case of *United States v. Nicaragua* highlighted the distinction between activity that would be an impermissible use of force under Article 2(4) but would not rise to the level of an *armed attack*, and that which would permit military action under Article 51's inherent right of self-defense.[8] The cyber domain allows a state to conduct operations that fall below the use of force, as well as operations that might cause destruction to property or injury and death to persons. Cyber activity that causes death, injury, or property damage *could* rise to the level of a use of force or armed attack under international law.

As described by U.S. Cyber Command, cyber activity can be viewed along a spectrum of actions ranging from cyber espionage to access operations, and ultimately, on the far end of the spectrum, activity causing death or the destruction of property (see figure).[9]

Cyber espionage, for example, would not amount to the impermissible use of force or armed attack triggering the right of the offended state to respond in self-defense because the result is simply theft or access to another state's networked systems. Further along the spectrum, cyber disruption operations likewise would fall short of an unlawful use of force. For instance, disruption opera-

tions that involve accessing another state's networked systems and interfering with the operations of the network could violate the principle of nonintervention. This principle is grounded on the premise that states are prohibited from interfering in the internal affairs of other states. An aggrieved state may protest such activity through the UN Security Council, but simply accessing and manipulating data would not justify an armed response under customary international law or Article 51. The far right of the spectrum in the cyber domain is the use of force/armed attack through cyber operations. The threshold standard justifying the invocation of self-defense under Article 51 and customary international law is high. The cyber activity must result in either physical destruction of property or death or injury of persons through sufficient scale and effect to meet the definition of an armed attack justifying a proportional response in self-defense.[10]

The closest open-source example of use of force in cyberspace is the Stuxnet virus, which was introduced into Iranian nuclear facilities and essentially damaged the centrifuges used to enrich uranium.[11] This example is intriguing because what is known about the operation involved exclusively computer-based means to cause the physical destruction of a state's critical infrastructure. Of course, how a victim state qualifies "action" as either a use of force, armed attack, or some other activity interfering with the sovereignty of the state is an essential step in justifying countermeasures or, in the extreme, a military response. The fact that the Iranian government downplayed the damage and impact of Stuxnet lessened the likelihood that the activity would be subject to an armed response in self-defense.

Despite arguments to the contrary, the application of jus ad bellum in cyber space is compatible with the traditional approach under international law. Matthew Waxman argues persuasively that cyber activity is not unlike any other novel weapon introduced in the international community. Furthermore, by applying an effects-based approach to cyber activity, operations in cyberspace should be judged by whether the *effect* of the cyber activity is tantamount to a prohibited use of force or military attack.[12] For example, if a certain cyber operation results in the physical destruction of critical infrastructure of another state, then the activity could be characterized as a use of force. Such activity might constitute an armed attack under international law if the force used were significant in the scale and effect against another state.[13]

The question of what activity rises to the level of a prohibited use of force under Article 2(4) and whether that activity constitutes an armed attack has been subject to differing international interpretations in the context of conventional weapons. Cyber activity certainly provides unique tools for states to employ against other states in furthering national security goals. However, by applying the law as it exists today (*lex lata)* to an effects-based approach to cyber operations, states have a basis for characterizing the nature of the activity in order to determine what lawful responses are available.

Cyber Activity and *Jus in Bello*

The *jus in bello* is the law applied in war. The LOAC presupposes that an armed conflict exists. At that point, the jus in bello regulates violence in the conduct of military operations. Armed conflict is one of two varieties, international armed conflict or noninternational armed conflict. As Gary Solis notes in *The Law of Armed Conflict: International Humanitarian Law in War*, the conflict status is critical to determine what law applies.[14] In an *international armed conflict*, defined as armed conflict between two or more states, the entire body of Geneva Law (Four Geneva Conventions of 1949 and Additional Protocol I) and Hague Law governing armed conflict would apply. However, in a *noninternational armed conflict*, defined as armed conflict between a state and an organized armed group, Common Article 3 of the Geneva Conventions, and, in certain circumstances, Additional Protocol II applies.[15] While the cyber domain is novel in the tools available to warfighters, the current law is sufficient to govern activity in the cyber domain within the context of an armed conflict, be it international or noninternational.

Department of Defense policy is to comply with the

U.S. Air Force (Jorge Intriago)

Air National Guardsman uses ROVER 5 handheld portable transceiver to view targeting data while performing close air support

Soldier attempts to set up connection with call manager during exercise Cyber Endeavor, Grafenwoehr, Germany

U.S. Army (Shawnon Lott)

LOAC no matter how an armed conflict is characterized and in all other military operations.[16] The four core principles of LOAC are military necessity, distinction, proportionality, and unnecessary suffering. Cyber activity conducted during an armed conflict is governed by the same rules as other capabilities that a military force may use to ensure accomplishment of a unit's mission. However, prior to analyzing cyber activity within the framework of the four core principles, the first question that must be answered is whether the cyber activity constitutes an "attack" under the LOAC.

Attack is defined in Article 49 of Additional Protocol I as "acts of violence against the adversary, whether in offense or defense."[17] Michael Schmitt emphasizes in his article on "Cyber Operations and the Jus in Bello" that violent action is required to constitute an attack.[18] Cyber operations during armed conflict certainly could result in "violent actions" triggering the same legal and operational analysis of the four core principles as any weapon or capability within a state's arsenal. However, as discussed in the jus ad bellum analysis of sub-uses of force in the cyber domain, it is easy to contemplate that most cyber activity would not reach the violent action standard. Cyber activity could certainly be used as a shaping action in conjunction with a much larger operation carried throughout the military domains of land, sea, air, and space. For example, cyber activity could be used to provide certain information to the civilian population within the battlespace in the course of information operations. The target is the civilian population, but if the sole purpose, and more importantly, the *effect* of the cyber activity is simply to influence and provide information favorable to U.S. military operations, the activity would not constitute an attack and the four core principles are not implicated.

A more difficult analysis lies in circumstances where there will be damage or destruction to civilian property. For civilian property to be subject to an attack, the principle of military necessity must be satisfied. *Military necessity* authorizes the use of force required to accomplish the mission. However, military necessity does not authorize acts otherwise prohibited by the law of war. Closely related to military necessity is the concept of *distinction*, which requires that attacks only be directed against military personnel and military objects. To satisfy this principle, cyber activity must be attributed to a state or nonstate actor. The example of the Estonian DDOS activity is a classic problem of attribution. The Russian government claimed no responsibility and blamed the DDOS activity on "hacktivists," patriotic Russians who independently used cyber tools to influence a foreign state.[19] Attribution is certainly a significant problem in cyber operations; however, it is not insurmountable. Terrorist attacks and military operations conducted by insurgents sponsored by third-party states have raised attribution problems in the past. Existing resources can address the attribution problems in the cyber domain. Detailed intelligence, coupled with the experience and judgment of the responsible commander, are just as applicable in the cyber domain as in other areas of military operations.

Once a target is identified, it must meet the requirement of being a *valid military objective*, defined in Additional Protocol I as an object that by its nature, location, purpose, or use makes an effective contribution to military action, and whose total or partial destruction, capture, or neutralization offers a definite military advantage.[20] Cyber operations may be directed against exclusively military objects or against so-called dual-use structures having both military and civilian purposes. Targeting dual-use objects must comply with the standards of military necessity and meet the definition of a valid military objective.

A unique aspect of operating in the cyber domain is the simple fact that much of the infrastructure subject to attack also supports the civilian population. The concept of proportionality becomes critical to determining the lawfulness of cyber operations that result in the physical destruction of dual-use targets. The principle of *proportionality* states that the anticipated loss of civilian life and damage to civilian property incidental to an attack must not be excessive in relation to the concrete and direct military advantage expected.[21] Dual-use structures such as radio transmission towers, power lines, and oil refinery stations are some of the most difficult targeting decisions to work through because of the effect their destruction will have on the civilian population.

Dual-use targets in the context of cyberwar are further complicated when the target is data contained on a network server. It is easy to imagine how certain data that aid enemy operations would meet the definition of a valid military objective. Also easy to imagine is how that same data could aid the civilian population. Professor Schmitt argues that data should not generally be characterized as an object in itself in the cyber domain unless its destruction causes the requisite level of harm.[22] For example, destroying the entire banking system of a state may severely affect the civilian population. Additionally, destroying digital art would be analogous to destroying tangible art. Some attacks in the cyber domain would clearly be impermissible (targeting digital art), while others would only be permissible if there were articulable military necessity or operations could distinguish between the valid military objective and civilian objects. In the case of dual-use targets, the principle of proportionality would have to be satisfied. Cyber operations do present a unique opportunity to specifically

target certain aspects of a dual-use structure through methods that would easily satisfy the principle of proportionality. For example, the Stuxnet virus was specific as to which components of the centrifuges would be affected and what harm would result. If given the option to "destroy" a target using cyber methods that carefully calculate the anticipated damage to the surrounding area, clearly that method would be preferable to dropping a bomb on the target causing substantially more damage and potentially resulting in greater collateral effects. It is important to keep in mind that such operations resulting in the "destruction" of infrastructure—and in limited circumstances, data—are at the extreme end of the spectrum of cyber operations. The vast majority of operations discussed in open-source reporting involve a sub-use of force. Operations that focus on accessing data, influencing the civilian population through information operations, or disrupting cyber capabilities will generally not reach the threshold of a "use of force" or "attack" as currently defined.

Finally, cyber operations must avoid causing *unnecessary suffering* to combatants. The LOAC principle of unnecessary suffering (commonly referred to as *superfluous injury*) recognizes that the harm caused even to combatants should not be unlimited. The LOAC proscribes certain means and methods of warfare designed to cause suffering to combatants that is substantially disproportional to the military advantage.[23] Examples of means or methods that cause superfluous injury include poison gases, certain exploding bullets, and glass fragmentation devices that preclude identifying and treating wounds by X-ray. Lawful weapons can also be used in a manner that violates the principle of unnecessary suffering. Incendiary devices used for marking and screening in military operations, if used with the intent of causing unnecessary suffering by burning combatants, is one often-cited example. Cyber tools must be treated no differently than any other weapon system. Cyber tools and activity are not likely to trigger a prohibition per se, as have poison gases and blinding lasers; however, the effects of the cyber tool must still be considered against the core principle of unnecessary suffering. Cyber tools have the unique advantage of not only mitigating the effects on the civilian population, but also more completely taking into account the effects on combatants and steering clear of any effects that cause unnecessary suffering under the LOAC.

Conclusion

The threat to U.S. national security in the cyber domain is real, but is the cyber sky falling? A discussion of all cyber threats facing the United States is beyond the scope of this article. Obvious challenges exist in the cyber domain, to include attributing cyber activity to a specific state or nonstate actor and the speed of action in the cyber domain. Both attribution and speed of action complicate the decisionmaking process and effectiveness of existing countermeasures. However, what is apparent is that within the context of jus ad bellum and jus in bello, the current framework is adequate to navigate through the *operational* issues facing military professionals. From an operational perspective, cyber is simply one of five domains (land, sea, air, space, and cyber) that commanders must understand, plan, and operate in to accomplish the assigned mission. Similar to the introduction of airplanes and submarines in a commander's battlespace, cyber tools can be regulated using existing laws governing the use of force and military operations. The advantage of cyber tools exists in the potential to control the effects during an attack that could dramatically reduce the collateral damage associated with targeting military objectives. **JFQ**

the effects of the cyber tool must still be considered against the core principle of unnecessary suffering

NOTES

[1] General James E. Cartwright, USMC, Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, and Directors of the Joint Chiefs Directorates, "Joint Terminology for Cyberspace Operations" n.d., 7.

[2] David T. Fahrenkrug, "Cyberspace Defined," available at <www.au.af.mil/au/awc/awcgate/wrightstuff/cyberspace_defined_wrightstuff_17may07.htm>.

[3] Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010), 13–14.

[4] Ibid., 15–16.

[5] Ibid., 1–3.

[6] Sean Condron, "The Legal Basis for the Use of Force," *Operational Law Handbook* (Charlottesville, VA: The Judge Advocate General's Legal Center and School, 2011), 1.

[7] Brian J. Brill and J. Porter Harlow, *Law of War Documentary Supplement* (Charlottesville, VA: The Judge Advocate General's Legal Center and School, 2010), 1.

[8] International Court of Justice (ICJ), *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment of June 27, 1986, LEXIS 4.

[9] Paul Walker, "Assessing Actions Along the Spectrum of Cyberspace Operations," PowerPoint briefing at the James Stockdale Center for Ethical Leadership, Annapolis, February 29, 2012.

[10] Tom Ruys, *Armed Attack and Article 51 of the UN Charter* (Cambridge: Cambridge University Press, 2010), 140.

[11] Gary D. Solis, "Cyberwarfare, the New Normal," *The Law of Armed Conflict: International Humanitarian Law at War*, 2nd ed. (New York: Cambridge University Press, 2012).

[12] Matthew C. Waxman, "Cyber Attacks as 'Force' under UN Charter Article 2(4)," *International Law Studies* 87; Raul A. Pedrozo and Daria P. Wollschlaeger eds., *International Law and the Changing Character of War* (Newport, RI: U.S. Naval War College, 2011).

[13] See *Nicaragua v. United States*; also *Oil Platforms Case* (2003 ICJ LEXIS 11).

[14] Solis, 149.

[15] Ibid., 167–168.

[16] Condron, citing Department of Defense Directive 2311.01E, "DoD Law of War Program," para. 4.1.

[17] Brill and Harlow, 210.

[18] Michael N. Schmitt, "Cyber Operations and the Jus in Bello: Key Issues," *International Law Studies* 87, 92–93.

[19] Clarke, 15–16.

[20] Condron, 12.

[21] Brill and Harlow, 211.

[22] Schmitt, 96.

[23] Solis, 272.